FEP PIA

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of System: Front End Processor

(b) Bureau: Consular Affairs

(c) System Acronym: FEP

(d) iMatrix Asset ID Number: 344

(e) Reason for Performing PIA:

☐ New System

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒ Yes

☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security assessment and authorization (A&A) status of the system?

FEP received an Authorization to Operate in July 2013 for a period of 36 MONTHS.

The triennial Assessment and Authorization process is underway and FEP is expected to receive an Authorization-To-Operate by December 2016.

(c) Describe the purpose of the system:

The FEP system consists of four application servers and two Structured Query Language (SQL) Server databases located on the State Department unclassified intranet. FEP provides mission-critical support for timely and accurate translation of data requests between Passport Systems' major applications. FEP is a multi-threaded application that provides the Travel Document Issuance System (TDIS), Passport Record Imaging System Management (PRISM), American Citizen Services (ACS), Consular Lookout and Support System (CLASS), Passport Information Electronic Records System (PIERS) and Passport Lookout Tracking System (PLOTS) applications the ability to communicate with several database systems and to interface with Department of Homeland Security Customs and Border Protection (DHS/CBP) via SQL Server Integration Services (SSIS) 2008 packages. FEP does not generate or save any new data. Its only function is to perform accurate data translation. For every data request and translation, there is a transaction record entered into the FEP database server.

The FEP Automated Information System (AIS) performs the following functions:

- Namecheck Service (CLASS, In-Process Database, and Multiple Issuance Verification queries)
- Social Security Administration (SSA) Service (checks the validity of the Social Security numbers and the Death Master File)
- Consular Lost and Stolen Passport System (CLASP) and CLASS (adds, updates, and queries)
- Signature Delivery Service (Passport book chip)
- CA XML (Extensible Markup Language) Translation
- Image Retrieval – requested by SQL Server Database SSIS package. The image and the passport applicant's PII data (XML data) is then written to the Oracle DataShare Database. Additional validations are performed by the Oracle DataShare leg. The applicant's Image and PII data is then sent from the Oracle DataShare database to DHS/CBP

- Load balancing and failover support across client systems

An additional component to the FEP is the ESB (Enterprise Service Bus) Re-director. The ESB Re-director is a temporary initiative by the Department of State's Office of Consular Systems and Technology (CST) to facilitate the migration of the FEP Services to the ESB. The ESB Re-director is a proxy service that routes incoming queries from systems (Travel Document Issuance System, American Citizen Services, and Passport Lookout Tracking System) to the ESB for namecheck service as they become available for use on the ESB.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

FEP processes the following personally identifiable information (PII) elements when Passport Agencies and Department of State employees use the FEP system for executing queries and other transactions:

Names of Individuals
Birthdates of Individuals
SSN or other identifying numbers
Individual ID numbers from other sources
Personal Address
Phone number(s) of Individuals
e-mail address(es) of individuals
Images or Biometric IDs and other individually identifying items

The PII is maintained on-line in transaction logs for a period of two weeks. After that, the logs are permanently archived off-line by State Department Enterprise Operations.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended);
18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure);
22 U.S.C. 211a-218, (Passports)
22 U.S.C. 2651a (Organization of Department of State);

Executive Order 11295, August 5, 1966, 31 FR 10603; (Authority of the Secretary of State in granting and issuing U.S. passports);
8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
26 U.S.C. 6039E (Information Concerning Residence Status)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒ **Yes, provide:**

SORN Name and Number:
SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
State-05 Overseas Citizens Records, May 2, 2008
State-26 Passport Records, March 24, 2015

☐ **No, explain how the information is retrieved without a personal identifier.**

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?

☐ Yes
☒ No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?

☐ Yes
☒ No

FEP does not generate or save any new data. Its only function is to perform accurate data translation. For every data request and translation, there is only a transaction record entered into the FEP database server.
~~The Bureau of Consular Affairs (CA) maintains the data within its systems indefinitely, until a records disposition schedule is approved by NARA in partnership with the Bureau of Administration (A). Currently, CA and A Bureau are coordinating to revise records~~

Comment [CDB1]: Are these records automatically deleted after two weeks?

~~schedules for CA systems. Until the records disposition schedules are approved by NARA, the records will be maintained indefinitely.~~

Comment ["2]: The way the document reads, it seems as though FEP doesn't store data. Is that the case? If so, revise this answer.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- ☒ Members of the Public
- ☐ U.S. Government employees/Contractor employees
- ☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- ☒ Yes
- ☐ No

If yes, under what authorization?

26 U.S.C. 6039E – Information Concerning Resident Status

(c) How is the information collected?

FEP receives and transmits electronic transactions containing PII to and from several Consular Affairs systems via the State Department intranet. FEP does not originate PII data, collect PII data, nor does it maintain any PII data in long term storage.

(d) Where is the information housed?

- ☒ Department-owned equipment
- ☐ FEDRAMP-certified cloud
- ☐ Other Federal agency equipment or cloud
- ☐ Other

If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

Data processed by FEP is sourced from several systems. FEP is totally dependent upon the validity, safeguards, and accuracy of the sourcing data systems.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

FEP receives and transmits transactions containing PII to and from several Consular Affairs systems. FEP does not update or check for accuracy. It is up to the applicant entering the information in the other CA information systems to ensure that the information entered is current. The applicant is responsible for updating the information for the record in accordance with the procedures stated in the relevant System of Records Notice (SORN), if the applicant so chooses to update the record.

(g) Does the system use information from commercial sources? Is the information publicly available?

FEP does not use commercial information or publicly available information.

(h) Is notice provided to the individual prior to the collection of his or her information?

FEP only processes transactions containing PII data that is collected by other Consular Affairs systems. FEP does not collect PII data directly from any users.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?

☐ Yes

☒ No

If yes, how do individuals grant consent?

If no, why are individuals not allowed to provide consent?

FEP only processes transactions containing PII data that is collected by other Consular Affairs systems.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

As the system processes sensitive information, FEP does not collect data and only maintains it in transaction logs for two weeks. ~~The primary risk/concern is misuse by an authorized FEP System Administrator tampering with the system to extract PII from the FEP transaction stream. Misuse may result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised, administrative burdens, financial loss, loss of public reputation and confidence, and civil liability for the Department of State~~

Comment [CDB3]: I think this can go.

5. Use of information

(a) What is/are the intended use(s) for the information?

The FEP system is an application that provides a communications interface to various front-end client applications for executing queries and other transactions with back-end systems and/or databases. It serves as a controller/director where data requests from one application (client) are redistributed to various application systems (clients/servers). It consists of an engine that matches data front-end queries to the backend databases. The PII is maintained on-line in transaction logs for a period of two weeks. After that, the logs are permanently archived off-line by State Department Enterprise Operations. PII is retained for reference during any investigations involving breach of security or misuse of government systems.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the use of the information by FEP is relevant to the purpose for which the system was designed.

(c) Does the system analyze the information stored in it?

☐ Yes

☒ No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record?

☐Yes

☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

☐Yes

☒No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

FEP shares information *internally* with:

- FEP prepares and drops batches of data to Consular Data Information Transfer System (CDITS) for transfer to outside agencies.
- For requesting systems, FEP retrieves images of passports scanned and stored by Passport Record Imaging System Management (PRISM);
- Travel Document Issuance System (TDIS) runs name checks through FEP and uses FEP to get digital signatures for ePassports:
- Passport Lookout Tracking System (PLOTS) uses FEP for image retrieval and for CLASS adds, deletes, and queries;
- American Citizen System (ACS) runs name checks through FEP; and
- Information shared between Consular Lookout and Support System (CLASS) and FEP is for the purpose of name check and confirmation.

FEP information is not shared *externally* with entities outside of the Department of State.

(b) What information will be shared?

FEP transmits names of individuals, birthdates of individual, SSNs, phone numbers of individuals, email addresses, and images or biometric IDs.

(c) What is the purpose for sharing the information?

The FEP provides mission-critical support for timely and accurate translation of data requests between Passport Systems major applications within Consular Affairs. FEP information is not shared *externally* with entities outside of the Department of State.

(d) The information to be shared is transmitted or disclosed by what methods?

Internally, FEP serves as a robust, timely, and accurate data broker, controller, and director which interacts directly with CA Information Systems over the Department of State intranet via. SQL data packets. FEP data is not *externally* shared or disclosed so there are no additional privacy risks.

(e) What safeguards are in place for each internal or external sharing arrangement?

Information is shared *internally* by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. For every data request processed by FEP, a full record of the data transaction is entered into the FEP database server transaction logs. FEP data is not *externally* shared or disclosed so there are no additional privacy risks.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

FEP receives a request from CA Information Systems which will require it to collect, translate, and then transmit PII back to FEP and then finally the requesting CA Systems. To address the concerns of transmitting PII the data is turned into a machine readable only language (SQL language) and then forwarded onto the requesting CA Systems.

~~Human users are the primary threat vector associated with the risk of unauthorized disclosure of privacy information. Individuals may execute queries in FEP in order to gain access to information that they do not have a need to know. As such, individuals are only able to query systems that directly correspond to their area of responsibility. Additionally, required management, operational and technical controls are verified annually to be in place to reduce and mitigate this risk, including required annual security training, separation of duties, rigorous application of least privilege, access badges, and personnel background screening.~~ FEP data is not *externally* shared or disclosed so there are no additional privacy risks.

Comment [CSL4]: There appears to be two thoughts here that seem to contradict each other.

Comment ["5]: Feel free to reword and keep only if applicable. This is a way to answer the question to make it specific to the system.

Comment [BAF6]: This sentence is not needed.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

FEP only processes transactions containing PII data that is collected by other Consular Affairs systems. The systems sourcing the data to FEP have the responsibility for meeting this requirement.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☐ Yes

☒ No

If yes, explain the procedures.

If no, explain why not.

FEP only processes transactions containing PII data that is collected by other CA systems. The systems sourcing the data to FEP have the responsibility for meeting this requirement.

(c) By what means are individuals notified of the procedures to correct their information?

FEP only processes transactions containing PII data that is collected by other CA systems. The systems sourcing the data to FEP have the responsibility for meeting this requirement.

8. Security Controls

(a) How is the information in the system secured?

The FEP application data is protected by multiple layers of security controls including OpenNet security, FEP application security, Department site physical security and management security.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Access to the FEP application is restricted to cleared, authorized Department of State FEP System and Database Administrators ~~via the Department unclassified intranet~~. To

access the system, administrators must be an authorized user of the Department of State's unclassified network. Each authorized administrator must sign a user access agreement before being given an account with FEP administrator privileges. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon and "need to know" access for perform their specific job responsibilities. ~~System administrators can access the FEP application only at the central server location to perform application maintenance tasks, such as installation of patch updates or modification of the system's customized software functionality.~~ External access to any non-Department entity is strictly prohibited.

~~Personnel accessing FEP information must be authorized by FEP management. Authorized personnel require a user ID and password to access FEP information. User access to FEP information is restricted to administrator roles only.~~

~~Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.~~=

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The system's automatically generated audit trails ~~that are automatically generated~~ are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.)

(d) Explain the privacy training provided to authorized users of the system.

In accordance with Department of State computer security policies, FEP administrators are required to attend a security briefing and complete the Department of State's Cyber Security Awareness Training prior to receiving access to the system. In order to retain the access the administrators must complete annual refresher training. For those that handle PII, ~~role based~~ privacy t~~PII T~~raining provided by Department of State must be completed at least once a year. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users must protect PII through appropriate safeguards to ensure security, privacy and integrity. These Rules of Behavior are included in the annual privacy training.

Comment ["7"]: *Explain the different roles that have been created to provide access to the system* This response refers to OpenNet access which applies to most systems. This is baseline restriction on access. If you'd like to include, please shorten it to a sentence or two.

The subsequent paragraph answers the question, but please mention the procedures (i.e. – who determines/clears on the roles). To confirm, the only role that has access is admin?

Comment [BAF8]: There are System Admins and Database Admin roles only.

Comment [CDB9]: PA459 isn't role based

Comment ["10"]: Is this an office administered training or PA459?

Comment [BAF11]: Department of State Mandatory training.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?

☒ Yes
☐ No

If yes, please explain.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and reporting, identification and authentication of organizational users, Information System Monitoring and numerous Media Controls.

(f) How were the security measures above influenced by the type of information collected?

The information collected contains PII of U.S. Citizens and Legal Permanent Residents (LPR). The measures implemented are the result and consideration of the amount and type of PII that is collected. Due to the sensitivity of the information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing. ~~The information collected contains PII of U.S. Citizen and Legal Permanent Residents (LPR).~~

9. Data Access

(a) Who has access to data in the system?

Only authorized FEP System Administrators have access to and process transactions containing PII data that is collected by other Consular Affairs systems.

(b) How is access to data in the system determined?

Access to the FEP application is restricted to cleared, authorized Department of State FEP System and Database Administrators. To access the system, administrators must be an authorized user of the Department of State's unclassified network. Each authorized administrator must sign a user access agreement before being given an account with FEP

Comment ["12]: *criteria, procedures, responsibilities*

What criteria allows individuals to gain access? What are the procedures to gaining that access (I see that FEP mgmt. has to authorize. Anything else)? Is access determined by responsibilities? If so, what are they?

Comment [BAF13]: I think this answer is sufficient

administrator privileges. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon and "need to know" access for perform their specific job responsibilities.~~Access to the FEP application is restricted to cleared, authorized Department of State FEP System Administrators via the Department's unclassified intranet. To access the system, administrators must be an authorized user of the Department of State's unclassified network. Each authorized administrator must sign a user access agreement before being given an account with FEP administrator privileges. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. System administrators can access the FEP application only at the central server location to perform application maintenance tasks, such as installation of patch updates or modification of the system's customized software functionality. External access to any non-Department entity is strictly prohibited.~~

~~Personnel accessing FEP information must be authorized by FEP management. Authorized personnel would first require a network account that would be logged into utilizing their Common Access Card (CAC) and PIN and then they would use a user ID and password to access the FEP application. User access to FEP information is restricted to administrator roles only.~~

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

☒ Yes
☐ No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Personnel accessing FEP information must be authorized by FEP management. Authorized personnel require a user ID and password to access FEP information. User access to FEP information is restricted to administrator roles only.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

~~These risk factors are mitigated through the use of Technical, Management, and Operational security controls.~~ ~~The~~ FEP application data is protected by multiple layers of security controls including OpenNet security, FEP application security, Department site physical security and management security. Specifically access controls, identification and authentication controls, audit controls, and awareness and training controls are implemented to reduce the risk of users authorized to access system data from performing unauthorized actions.

~~All privacy controls: Authority and Purpose (AP), Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI), Data Minimization and Rentention (DM), Individual Participation and Redress (IP) Security (SE), Transparency (TR), and Use Limitation (UL). Also Access Control (AC), Audit and Accountability (AU), Identification and Authentication (IA), System and Communications Protection (SC), Awareness and Training (AT), Media Protection (MP), Personnel Security (PS) and Configuration Management (CM).~~
~~Personnel accessing FEP information must be authorized by FEP management. Authorized personnel would first require a network account that would be logged into utilizing their Common Access Card (CAC) and PIN and then they would use a user ID and password to access the FEP application. User access to FEP information is restricted to administrator roles only. Additionally, the use of audit trails help deter the misuse of data.~~

Comment ["14]: What risk factors??

Comment ["15]: This doesn't tell us what those controls are.

Comment [BAF16]: All privacy controls: AP, AR, DI, DM, IP SE, TR, and UL. Also AC, AU, IA, SC, AT, CM